

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2001-256113
(P2001-256113A)

(43) 公開日 平成13年9月21日 (2001.9.21)

(51) Int.Cl. ⁷	識別記号	F I	テ-リ-ト (参考)
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 A 5 B 0 1 7

審査請求 未請求 請求項の数14 O L (全 12 頁)

(21) 出願番号 特願2000-69262(P2000-69262)

(22) 出願日 平成12年3月13日 (2000.3.13)

(71) 出願人 000003078

株式会社東芝

東京都港区芝浦一丁目1番1号

(72) 発明者 石橋 泰博

東京都青梅市末広町2丁目9番地 株式会
社東芝青梅工場内

(74) 代理人 100058479

弁理士 鈴江 武彦 (外6名)

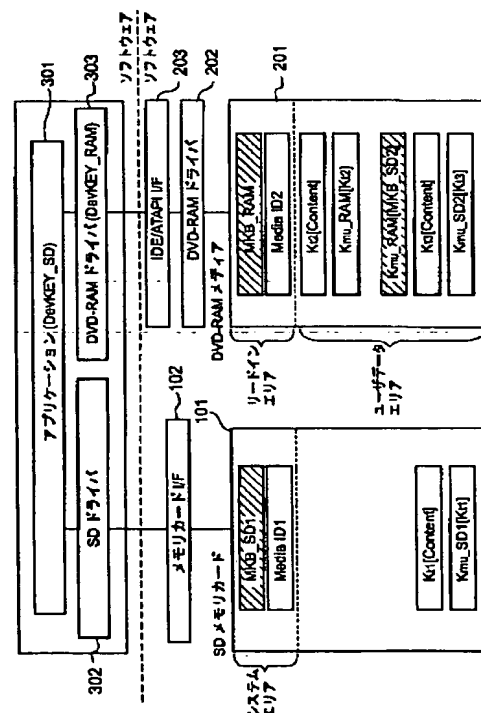
Fターム(参考) 5B017 AA01 BA02 BA05 BA07 BB02
BB06 CA09 CA14 CA16

(54) 【発明の名称】 コンテンツ処理システムおよびコンテンツ保護方法

(57) 【要約】

【課題】ある特定のメディア種別に対応したデバイス識別情報によって他のメディア種別の記録メディアを扱う。

【解決手段】DVD-RAMドライバ303のインストール時には、SDメモ리카ード用の最新のメディアキーブロック (MKB_SD2) がWEBサーバやDVD-RAMドライバ303用のインストールCDなどから取得され、それがDVD-RAMメディア201のユーザデータエリアに書き込まれる。アプリケーションプログラム301からのDVD-RAMメディア201に対する認証要求があると、DVD-RAMメディア用のメディアキーブロック (MKB_RAM) の代わりに、SDメモ리카ード用の最新のメディアキーブロック (MKB_SD2) がDVD-RAMメディア201から読み出され、それがアプリケーションプログラム301に渡される。



【特許請求の範囲】

【請求項1】 記録メディアに予め記録された、排除すべき電子機器のデバイス識別情報を特定可能なリボケーションリスト情報と、前記記録メディアを扱う電子機器のデバイス識別情報とを用いて、前記記録メディアと電子機器間の認証を行うコンテンツ処理システムであって、

前記デバイス識別情報およびそれに対応する前記リボケーションリスト情報は、記録メディアの種別毎に異なっており、

第1のメディア種別に対応するリボケーションリスト情報に対応した第1のデバイス識別情報を有する電子機器で第2のメディア種別の記録メディアを扱う場合、前記第2のメディア種別の記録メディアに対応した制御プログラムによって、前記第1のメディア種別に対応するリボケーションリスト情報を前記第2のメディア種別の記録メディア上に記録させる手段を具備することを特徴とするコンテンツ処理システム。

【請求項2】 前記第1のデバイス識別情報を有する電子機器上で動作するコンテンツ処理プログラムから前記第2のメディア種別の記録メディアに対する認証要求が発行された場合、前記第2のメディア種別の記録メディアに対応するリボケーションリスト情報に代えて、前記第1のメディア種別に対応するリボケーションリスト情報を前記第2のメディア種別の記録メディアから読み出して前記コンテンツ処理プログラムに渡す手段をさらに具備することを特徴とする請求項1記載のコンテンツ処理システム。

【請求項3】 前記制御プログラムは、前記第2のメディア種別の記録メディアをリード／ライト制御するドライブ装置用のデバイスドライバであることを特徴とする請求項1記載のコンテンツ処理システム。

【請求項4】 前記制御プログラムは、前記第1の第2のメディア種別に対応した第2のデバイス識別情報を有しており、その第2のデバイス識別情報と、前記第2のメディア種別の記録メディア上に予め記録されている第2のメディア種別に対応するリボケーションリスト情報とを用いて、前記第2のメディア種別の記録メディアとの認証を行い、正当なもの同士あることが確認された場合に、前記第1のメディア種別に対応するリボケーションリスト情報を前記第2のメディア種別の記録メディア上に記録することを特徴とする請求項1記載のコンテンツ処理システム。

【請求項5】 前記第1のメディア種別に対応するリボケーションリスト情報は、前記制御プログラムが前記第2のメディア種別の記録メディア上に予め記録されているリボケーションリスト情報との認証によって得た暗号化鍵によって暗号化された状態で、前記第2のメディア種別の記録メディア上に記録されることを特徴とする請求項4記載のコンテンツ処理システム。

【請求項6】 コンテンツ保護のために排除すべき電子機器のデバイス識別情報を特定するために記録メディアにあらかじめ記憶されたリボケーションリスト情報と、前記記録メディアを扱う電子機器のデバイス識別情報とを用いて、コンテンツ保護に必要な機能を持つ正当なもの同士であるか否かの認証を行い、その認証によって、コンテンツの暗号化／復号化を管理するための記録メディア固有キーを生成するコンテンツ処理システムであって、

前記デバイス識別情報およびそれに対応する前記リボケーションリスト情報は、記録メディアの種別毎に異なっており、

第1のメディア種別に対応するリボケーションリスト情報に対応した第1のデバイス識別情報を有し、前記第1のメディア種別に属する第1の記録メディアとの間の認証によって得た第1の記録メディア固有キーを用いて、コンテンツの記録または読み出しを行うコンテンツ処理手段と、

前記コンテンツ処理手段によって前記第1のメディア種別とは異なる第2のメディア種別に属する第2の記録メディアを使用する場合、前記第1のメディア種別に対応するリボケーションリスト情報を前記第2の記録メディア上に書き込み、その書き込んだリボケーションリスト情報を前記コンテンツ処理手段からの認証要求に応じて前記コンテンツ処理手段に渡すことにより、前記コンテンツ処理手段と前記第2の記録メディアとの間の認証を実行させる制御手段とを具備することを特徴とするコンテンツ処理システム。

【請求項7】 前記第2の記録メディアには、前記第2のメディア種別に対応するリボケーションリスト情報があらかじめ記録されており、

前記制御手段は、前記第2の記録メディアにあらかじめ記録されているリボケーションリスト情報に対応した第2のデバイス識別情報を有し、前記第2の記録メディアとの間の認証によって得た記録メディア固有キーを用いて、前記第1のメディア種別に対応するリボケーションリスト情報を暗号化した後に前記第2の記録メディア上に書き込むことを特徴とする請求項6記載のコンテンツ処理システム。

【請求項8】 前記制御手段は、前記コンテンツ処理手段からの認証要求に応じて、前記第1のメディア種別に対応する前記暗号化されたリボケーションリスト情報を、前記第2の記録メディアとの間の認証によって得た記録メディア固有キーを用いて復号化した後に前記コンテンツ処理手段に渡すことを特徴とする請求項7記載のコンテンツ処理システム。

【請求項9】 前記制御手段は、前記第1のメディア種別に対応する最新のリボケーションリスト情報を外部から取得し、その取得したリボケーションリスト情報を前記第2の記録メディア上に書き込むことを特徴とする請

求項6または7記載のコンテンツ処理システム。

【請求項10】 前記制御手段は、前記第2のメディア種別の記憶メディアを扱うための記憶装置の制御を行うドライバプログラムであることを特徴とする請求項6記載コンテンツ処理システム。

【請求項11】 コンテンツ保護のために排除すべき電子機器のデバイス識別情報を特定するために記録メディアにあらかじめ記憶されたリボケーションリスト情報と、前記記録メディアを扱う電子機器のデバイス識別情報とを用いて、コンテンツ保護に必要な機能を持つ正当なもの同士であるか否かの認証を行い、その認証によって、コンテンツの暗号化／復号化を管理するための記録メディア固有キーを生成するコンテンツ処理システムであって、前記デバイス識別情報およびそれに対応する前記リボケーションリスト情報は、記録メディアの種別毎に異なっており、電子機器が有するデバイス識別情報では認証することができない別種別の第1のリボケーションリスト情報が予め記憶された第1の記憶メディアを使用する場合、前記電子機器が有するデバイス識別情報に対応したメディア種別用の第2のリボケーションリスト情報を取得して前記第1の記憶メディアに記憶する手段と、前記電子機器からの前記第1の記憶メディアに対する認証要求に応じて、前記第1の記憶メディアに書き込んだ前記第2のリボケーションリスト情報を前記電子機器に渡すことにより、前記電子機器と前記第1の記録メディアとの間の認証を実行させる手段とを具備することを特徴とするコンテンツ処理システム。

【請求項12】 コンテンツ保護のために排除すべき電子機器のデバイス識別情報を特定するために記録メディアにあらかじめ記憶されたリボケーションリスト情報と、前記記録メディアを扱う電子機器のデバイス識別情報とを用いて、コンテンツ保護に必要な機能を持つ正当なもの同士であるか否かの認証を行い、その認証によって、コンテンツの暗号化／復号化を管理するための記録メディア固有キーを生成するコンテンツ保護方法であって、前記デバイス識別情報およびそれに対応する前記リボケーションリスト情報は、記録メディアの種別毎に異なっており、電子機器が有するデバイス識別情報では認証することができない別種別の第1のリボケーションリスト情報が予め記憶された第1の記憶メディアを使用する場合、前記電子機器が有するデバイス識別情報に対応したメディア種別用の第2のリボケーションリスト情報を取得して前記第1の記憶メディアに記憶することを特徴とするコンテンツ保護方法。

【請求項13】 前記電子機器から前記第1の記憶メディアに対する認証要求が発行された場合、前記第1の記

憶メディアに書き込んだ前記第2のリボケーションリスト情報を前記電子機器に渡すことにより、前記電子機器と前記第1の記録メディアとの間の認証を実行させることを特徴とする請求項12記載のコンテンツ保護方法。

【請求項14】 コンテンツ保護のために排除すべき電子機器のデバイス識別情報を特定するために記録メディアにあらかじめ記憶されたリボケーションリスト情報と、前記記録メディアを扱う電子機器のデバイス識別情報とを用いて、コンテンツ保護に必要な機能を持つ正当なもの同士であるか否かの認証を行い、その認証によって、コンテンツの暗号化／復号化を管理するための記録メディア固有キーを生成するコンテンツ処理システムで使用可能なコンピュータプログラムが記録されたコンピュータ読み取り可能な記録媒体であって、前記デバイス識別情報およびそれに対応する前記リボケーションリスト情報は、記録メディアの種別毎に異なっており、前記コンピュータプログラムは、電子機器が有するデバイス識別情報では認証することができない別種別の第1のリボケーションリスト情報が予め記憶された第1の記憶メディアを使用する場合、前記電子機器が有するデバイス識別情報に対応したメディア種別用の第2のリボケーションリスト情報を取得して前記第1の記憶メディアに記憶するステップと、前記電子機器からの前記第1の記憶メディアに対する認証要求に応じて、前記第1の記憶メディアに書き込んだ前記第2のリボケーションリスト情報を前記電子機器に渡すことにより、前記電子機器と前記第1の記録メディアとの間の認証を実行させるステップとを具備することを特徴とする記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、画像データや音楽データなどの様々なデジタルコンテンツを扱うことが可能なコンテンツ処理システムおよびコンテンツ保護方法に関する。

【0002】

【従来の技術】近年、コンピュータ技術の発達に伴い、マルチメディア対応のパーソナルコンピュータ、セットトップボックス、プレイヤー、ゲーム機などの各種電子機器が開発されている。この種の電子機器は、記録メディアに格納された画像データや音楽データなどの様々なデジタルコンテンツを再生できるほか、インターネット等を通じてデジタルコンテンツをダウンロードして使用することもできる。

【0003】これらデジタルコンテンツは、例えばMP E G 2、MP 3といったデジタル符号化技術の採用により、品質を落とすことなくコピーしたり、ダウンロードすることができる。このため、最近では、著作権保護の観点から、このようなデジタルコンテンツを不正使用か

ら保護するための技術の必要性が叫ばれている。

【0004】

【発明が解決しようとする課題】そこで、最近では、メモリカードなどのリムーバブルメディアを中心に、正当な著作権保護機能を有する電子機器と記録メディアとの間でのみコンテンツの受け渡しを可能にするための認証および暗号化の仕組みが開発され始めている。

【0005】代表的な認証および暗号化技術としては、電子機器固有のデバイス識別情報と、記録メディア側に記録されるリボケーションリスト情報と称されるキーマトリクスとを用いて認証を行うことによって、不当な電子機器の排除と正当な電子機器に対する暗号化鍵の発行を行う仕組みが考えられている。この仕組みを用いることにより、出荷時に記録メディアに記録するリボケーションリスト情報のみを最新のものに更新することだけで、ハッキングされたことが発覚したデバイス識別情報についてはその使用を無効化できるようになり、不正な攻撃からコンテンツを保護すること可能となる。

【0006】リボケーションリスト情報は、そのデータサイズが大きいくほど、排除可能なデバイス識別情報の組み合わせを増やすことができることから、できるだけ大きなデータサイズに設定することが好ましい。

【0007】しかし、実際には、記録メディアの種別毎に記憶容量は大幅に異なるので、異なるメディア種間で共通サイズのリボケーションリスト情報を用いると、種々の弊害が生じることになる。たとえば、メモリカードのように記憶容量が比較的小さい記録メディアについては、リボケーションリスト情報を大きく設定しすぎると、ユーザデータエリアとして割り当てべきメモリサイズが圧迫されてしまうことになる。また、リボケーションリスト情報によって認証可能なデバイス識別情報の数は有限であるため、メディア種間で共通のリボケーションリスト情報を規定すると、割り当て可能なデバイス識別情報の数の不足等の事態を招くことになる。

【0008】一方、記録メディアの種別毎に個々にリボケーション情報およびそれに対応するデバイス識別情報を規定すれば、各記録メディア種別に最適なサイズのリボケーションリスト情報を使用することが可能となる。ところが、このようにすると今度は、パーソナルコンピュータなどのように種別の異なる様々な記録メディアを扱うことが可能な機器においては、記録メディア間の互換性に関して以下のような問題が生じることになる。

【0009】例えば、メモリカード用のデバイス識別情報が割り当てられている正当な機器上で動作するアプリケーションプログラムは、その機器のデバイス識別情報と使用するメモリカード上に予め記録されているリボケーションリスト情報とを用いて認証を行うことにより、そのメモリカード上のコンテンツを扱うことができる。しかし、メモリカード以外の記録メディア、例えばDVD-RAMメディアなどを扱う場合には、そのDVD-R

AMメディア上に予め記録されているリボケーションリスト情報はメモリカード用のデバイス識別情報では扱うことができないため、メモリカードからDVD-RAMメディアにコンテンツを移すなどの処理を行うことはできなくなる。よって、ユーザは、著作権保護機能に対応した正当なDVD-RAMドライブを新たに購入したとしても、実際にはDVD-RAMメディアをメモリカードと同様に扱うことはできない。これは、ユーザにとっては非常に不便なことである。

【0010】本発明は上述の事情に鑑みてなされたものであり、ある特定のメディア種別に対応したデバイス識別情報によって他のメディア種別の記録メディアを扱えるようにすると共に、さらに、著作権保護機能に対応した正当な記録メディアであればその種別を意識することなく、それら記録メディアを透過的に扱うこともできるコンテンツ処理システムおよびコンテンツ保護方法を提供することを目的とする。

【0011】

【課題を解決するための手段】上述の課題を解決するため、本発明は、記録メディアに予め記録された、排除すべき電子機器のデバイス識別情報を特定可能なリボケーションリスト情報と、記録メディアを扱う電子機器のデバイス識別情報とを用いて、記録メディアと電子機器間の認証を行うコンテンツ処理システムであって、前記デバイス識別情報およびそれに対応する前記リボケーションリスト情報は、記録メディアの種別毎に異なり、第1のメディア種別に対応するリボケーションリスト情報に対応した第1のデバイス識別情報を有する電子機器で第2のメディア種別の記録メディアを扱う場合、前記第2のメディア種別の記録メディアに対応した制御プログラムによって、前記第1のメディア種別に対応するリボケーションリスト情報を前記第2のメディア種別の記録メディア上に記録させる手段を具備することを特徴とする。

【0012】このように、第2のメディア種別の記録メディアに対応した制御プログラムによって第1のメディア種別に対応するリボケーションリスト情報を第2のメディア種別の記録メディア上に記録することにより、その記録したリボケーションリスト情報を用いて第2のメディア種別の記録メディアとの認証を実行させることが可能となるので、第1のメディア種別に対応したデバイス識別情報で、第2のメディア種別の記録メディアを扱うことができる。よって、著作権保護機能に対応した正当な記録メディアであればその種別を意識することなく、それら記録メディアを扱うことが可能となる。

【0013】この場合、前記第1のデバイス識別情報を有する電子機器上で動作するコンテンツ処理プログラムから前記第2のメディア種別の記録メディアに対する認証要求が発行された場合、前記第2のメディア種別の記録メディアに対応するリボケーションリスト情報に代え

て、前記第1のメディア種別に対応するリボケーションリスト情報を前記第2のメディア種別の記録メディアから読み出して前記コンテンツ処理プログラムに渡す手段を設けることにより、コンテンツ処理プログラムは、メディア種別の違いを全く意識することなく、第1及び第2のメディア種別を透過的に扱うことが可能となる。

【0014】また、前記制御プログラムとしては、前記第2のメディア種別の記録メディアをリード/ライト制御するドライブ装置用のデバイスドライバを使用することが好ましい。これにより、ユーザがそのドライブ装置を新たに購入して使用する場合でも、既存の他の記録メディアとの互換性を維持することが可能となり、既存の他の記録メディアに対応するコンテンツ処理プログラムによって異なる種別の記録メディアを透過的に扱うことが可能となる。

【0015】また、前記制御プログラムは、前記第1の第2のメディア種別に対応した第2のデバイス識別情報を有しており、その第2のデバイス識別情報と、前記第2のメディア種別の記録メディア上に予め記録されている第2のメディア種別に対応するリボケーションリスト情報とを用いて、前記第2のメディア種別の記録メディアとの認証を行い、正当なもの同士あることが確認された場合に、前記第1のメディア種別に対応するリボケーションリスト情報を前記第2のメディア種別の記録メディア上に記録することを特徴とする。これにより、第1のデバイス識別情報のみの機器であっても、内部的に第2のメディア種別の記録メディアとの認証を行うことができるので、コンテンツをより安全に管理することが可能となる。

【0016】また、前記第1のメディア種別に対応するリボケーションリスト情報は、前記制御プログラムが前記第2のメディア種別の記録メディア上に予め記録されているリボケーションリスト情報との認証によって得た暗号化鍵によって暗号化した状態で、前記第2のメディア種別の記録メディア上に記録することが好ましい。これにより、前記第1のメディア種別に対応するリボケーションリスト情報を第2のメディア種別の記録メディアのユーザデータエリアに書き込んだ場合でも、その秘匿化を実現できる。

【0017】また、本発明は、コンテンツ保護のために排除すべき電子機器のデバイス識別情報を特定するために記録メディアにあらかじめ記憶されたリボケーションリスト情報と、前記記録メディアを扱う電子機器のデバイス識別情報とを用いて、コンテンツ保護に必要な機能を持つ正当なもの同士であるか否かの認証を行い、その認証によって、コンテンツの暗号化/復号化を管理するための記録メディア固有キーを生成するコンテンツ処理システムであって、前記デバイス識別情報およびそれに対応する前記リボケーションリスト情報は、記録メディアの種別毎に異なっており、第1のメディア種別に対応

するリボケーションリスト情報に対応した第1のデバイス識別情報を有し、前記第1のメディア種別に属する第1の記録メディアとの間の認証によって得た第1の記録メディア固有キーを用いて、コンテンツの記録または読み出しを行うコンテンツ処理手段と、前記コンテンツ処理手段によって前記第1のメディア種別とは異なる第2のメディア種別に属する第2の記録メディアを使用する場合、前記第1のメディア種別に対応するリボケーションリスト情報を前記第2の記録メディア上に書き込み、その書き込んだリボケーションリスト情報を前記コンテンツ処理手段からの認証要求に応じて前記コンテンツ処理手段に渡すことにより、前記コンテンツ処理手段と前記第2の記録メディアとの間の認証を実行させる制御手段とを具備することを特徴とする。

【0018】この構成においても、第1のメディア種別に対応したデバイス識別情報で、第2のメディア種別の記録メディアを扱うことが可能となるので、種別の異なる記録メディアを透過的に扱うことが可能となる。また、コンテンツの暗号化鍵としてメディア固有キーを用いているので、記録メディア単体で他の機器に移動して使用しても、移動先の機器が正当な機器であればコンテンツを再生することができる。

【0019】

【発明の実施の形態】以下、図面を参照して本発明の実施形態を説明する。

【0020】図1には、本発明の一実施形態に係るコンテンツ処理システムのシステム構成が示されている。このコンテンツ処理システムは画像データや音楽データなどの各種デジタルコンテンツを扱うためのものであり、たとえばパーソナルコンピュータ（PC）などの電子機器から構成されている。このコンテンツ処理システムにおけるコンテンツ保護の方法は、コンテンツを記録すべき記録メディア毎にその記録メディア固有のメディア固有キーを用いてコンテンツの暗号化/復号化を管理することを前提としている。これは、同一記録メディアであれば、その記録メディアを他のパーソナルコンピュータや電子機器で使用しても再生できるようにするためであり、コンテンツは各記録メディア毎にそのメディアとの認証によって個々に得られるメディア固有キーを用いて暗号化して記録される。

【0021】メディア固有キーを用いたコンテンツの暗号化/復号化の管理は、そのための専用機能を内蔵したコンテンツ処理用のアプリケーションプログラム301によって実行される。このアプリケーションプログラム301は、タンパ・レジスタント・ソフトウェアとして実現されている。タンパ・レジスタント・ソフトウェアとは、不正な内部解析や改竄などの攻撃に対して防衛機能を備えるソフトウェアを意味する。

【0022】本実施形態においては、コンテンツの記録・読み出しに使用される記録メディアとして、SD（Se

cure Digital) メモリカード101と、DVD-RAMメディア201が用いられる。SD (Secure Digital) メモリカード101のリード/ライトは、本電子機器に設けられたメモリカードインターフェース102と、SDカード制御用のデバイスドライバプログラムであるSDドライバ302を介して行われる。また、DVD-RAMメディア201のリード/ライトは、本電子機器に設けられたIDE/ATAPIインターフェース203に接続されるDVD-RAMドライブ202と、その制御用のデバイスドライバプログラムであるDVD-RAMドライバ303を介して行われる。

【0023】SDドライバ302およびDVD-RAMドライバ303もタンパ・レジスタント・ソフトウェアとして実現されている。

【0024】本実施形態では、これら記録メディアを用いたコンテンツの暗号化/復号化管理は、各記録メディアに予め記録されているリボケーションリスト情報と、電子機器毎に予め用意されるその電子機器固有のデバイス識別情報とを用いて行われる。

【0025】ここで、リボケーションリスト情報とは、コンテンツ保護のために排除すべき電子機器のデバイス識別情報の一覧が埋め込まれた認証用情報であり、認証相手となる電子機器のデバイス識別情報が無効化すべきものであるか否かの判定に使用されると共に、正当なデバイス識別情報であると判定された場合にはメディア固有キーの生成のために用いられる。このリボケーションリスト情報は多数のキーマトリクス情報から構成されおり、以下ではメディアキーブロック(MKB)と称することにする。正当な著作権保護機能を有すると認められた記録メディアは、メディアキーブロック(MKB)が記録された状態で出荷される。

【0026】デバイス識別情報は各電子機器毎に割り当てられる固有の識別情報であり、正当な著作権保護機能を有すると認められた電子機器にのみ発行される。各電子機器はデバイス識別情報が埋め込まれた状態で出荷される。以下では、デバイス識別情報をデバイスキー(Dev KEY)と称することにする。

【0027】メディアキーブロック(MKB)の内容は記録メディアの種別毎に異なっており、SD (Secure Digital) メモリカード101とDVD-RAMメディア201とは異なるメディアキーブロック(MKB)が用いられる。すなわち、SDメモリカード101には、SDメモリカード用に規定されたメディアキーブロック(MKB_SD1)が予め記録されており、またDVD-RAMメディア201には、DVD-RAMメディア用に規定されたメディアキーブロック(MKB_RAM)が予め記録されている。これらメディアキーブロックはそれぞれライトプロテクトされた読み出し専用領域、すなわちSDメモリカード101についてはシステムエリア、DVD-RAMメディア201についてはリ

ードインエリアに記録されている。

【0028】本実施形態の電子機器に割り当てられているデバイスキー(Dev KEY_SD)はSDメモリカード用のメディアキーブロックに対応するものであり、アプリケーションプログラム301はそのデバイスキー(Dev KEY_SD)を用いてSDメモリカード101との認証を行う。この認証によって正当なもの同士であることが認識されると、アプリケーションプログラム301は、認証結果により得られるメディアキーとSDメモリカード101固有の識別情報であるメディアID(Media ID1)とを用いて、SDメモリカード101に固有の暗号化鍵であるメディア固有キー(Kmu_SD1)を生成する。SDメモリカード101に記録するコンテンツの暗号化およびその復号化の管理は、メディア固有キー(Kmu_SD1)を用いて行われる。すなわち、アプリケーションプログラム301は、SDメモリカード101に以下のデータを書き込む。

【0029】・Kt1[Content]: タイトルキーKt1と称される秘密鍵によって暗号化されたコンテンツ

・Kmu_SD1[Kt1]: SDメモリカード101のメディア固有キー(Kmu_SD1)によって暗号化されたタイトルキー

なお、タイトルキーKt1としては例えば乱数などを用いた時変キーを利用することができる。

【0030】DVD-RAMドライバ303は、DVD-RAMメディアをSDメモリカードと同様に扱うための機能をアプリケーションプログラム301に対して提供する。アプリケーションプログラム301とDVD-RAMメディア201との認証、およびアプリケーションプログラム301によるDVD-RAMメディア201のリード/ライトは、すべてDVD-RAMドライバ303を介して行われる。

【0031】DVD-RAMドライバ303は、DVD-RAMメディア用のメディアキーブロック(MKB_RAM)に対応したデバイスキー(Dev KEY_RAM)を有しており、DVD-RAMメディア201との間の認証を行うことができる。さらに、DVD-RAMドライバ303には、以下の機能が含まれている。

【0032】・SDメモリカード用の最新のメディアキーブロック(MKB_SD2)をWEBサーバやDVD-RAMドライバ303用のインストールCDなどから取得し、それをDVD-RAMメディア201のユーザデータエリアに書き込む機能

・アプリケーションプログラム301からのDVD-RAMメディア201に対する認証要求に回答して、DVD-RAMメディア用のメディアキーブロック(MKB_RAM)の代わりに、SDメモリカード用の最新のメディアキーブロック(MKB_SD2)をDVD-RAM

Mメディア201から読み出して、アプリケーションプログラム301に渡す機能

これら機能の詳細は図4以降で詳述する。

【0033】(メディアキーブロック)次に、図2を参照して、メディアキーブロックとデバイスキーとの関係を説明する。前述したように、メディアキーブロックとデバイスキーは記録メディアの種別毎に個々に規定される。図2(A)はSDメモリカード用のメディアキーブロック(MKB__SD1)とデバイスキー(DevKEY__SD)の関係を示している。デバイスキー(DevKEY__SD)はそれぞれ16列のインデックス(INDEX)とそれに対応するキー情報(KEY)とから構成されており、メディアキーブロック(MKB__SD1)は16列×512行程度の暗号化されたキーマトリクス群から構成されている。デバイスキー(DevKEY__SD)の各列のインデックスの値はメディアキーブロック(MKB__SD1)上の参照位置を示すものであり、各インデックスと同一列で、そのインデックスの値で指定される行位置のキー情報が参照される。例えば、第1列のインデックス値が図示のように“1”の場合には、メディアキーブロック(MKB__SD1)上の第1列・第1行の位置が参照される。その位置には、デバイスキー(DevKEY__SD)の第1列のキー(ここでは“A”)によって暗号化されたメディアキーA[Km]、あるいはエラーコードA[Ec]が格納されている。エラーコードは、該当するデバイスキーが無効であることを意味する。16個のインデックスのいずれか一つによって、対応するキー情報(KEY)によって暗号化されたメディアキーを取得できれば、認証が成功したことになる。この構成により、最大で51216個のデバイスキーを無効化することができる。

【0034】図2(B)はDVD-RAMメディア用のメディアキーブロック(MKB__RAM)とデバイスキー(DevKEY__RAM)の関係を示している。デバイスキー(DevKEY__RAM)はそれぞれ16列のインデックス(INDEX)とそれに対応するキー情報(KEY)とから構成されており、メディアキーブロック(MKB__RAM)は、16列×2048行程度の暗号化されたキーマトリクス群から構成されている。これにより、メディアキーブロック(MKB__RAM)においては、最大で204816個のデバイスキーを無効化することができる。

【0035】(コンテンツの暗号化/復号化)次に、図3を参照して、記録メディアを用いて行うコンテンツの暗号化/復号化の原理について説明する。ここでは、SDメモリカードを例示して説明することにする。

【0036】<コンテンツ記録時>図3(A)はコンテンツ記録時の処理の流れを示している。まず、SDメモリカード用のメディアキーブロック(MKB__SD1)とSDメモリカード101に記録されているメディアキ

ーブロック(MKB__SD1)とを用いた認証処理が行われ(プロセス#1)、メディアキーKmが生成される。

【0037】このメディアキーKmとSDメモリカード101に記録されているメディアID(Media ID1)との演算処理(プロセス#2)により、メディア固有キー(Kmu__SD1)が生成される。次いで、所定のタイトルキーKtをメディア固有キー(Kmu__SD1)で暗号化する処理(プロセス#3)が実行され、これによってKmu__SD1[Kt]が生成される。また、記録対象のコンテンツに対してはタイトルキーKtによって暗号化する処理が施され(プロセス#4)、Kt[Content]が生成される。そして、Kmu__SD1[Kt]とKt[Content]がSDメモリカード101に記録される。

【0038】<コンテンツ再生時>図3(B)はコンテンツ再生時の処理の流れを示している。まず、SDメモリカード用のメディアキーブロック(MKB__SD1)とSDメモリカード101に記録されているメディアキーブロック(MKB__SD1)とを用いた認証処理が行われ(プロセス#5)、メディアキーKmが生成される。

【0039】このメディアキーKmとSDメモリカード101に記録されているメディアID(Media ID1)との演算処理(プロセス#6)により、メディア固有キー(Kmu__SD1)が生成される。次いで、暗号化されたタイトルキーKmu__SD1[Kt]を、メディア固有キー(Kmu__SD1)で復号する処理(プロセス#7)が実行され、これによってタイトルキーKtが得られる。また、暗号化されたコンテンツKt[Content]に対しては、それをタイトルキーKtによって復号する処理が施され(プロセス#8)、これによりContentが得られ、それが再生される。

【0040】(DVD-RAMドライブのインストール)次に、図4を参照して、SDメモリカード用の最新のメディアキーブロックMKB__SD2をDVD-RAMメディア201に書き込む処理について説明する。

【0041】この書込処理は、DVD-RAMドライブ303のインストール時にそのインストーラによって行われ、またインストール後はDVD-RAMドライブ303に付属するセットアッププログラムを起動することによって任意のタイミングで行うことができる。もちろん、書込処理を実行に当たっては、「DVD-RAMメディアをSDメモリカードと同等に扱う機能を追加しますか」というメッセージがユーザに提示され、ユーザから追加する旨の応答があった場合にのみ書込処理が実行されることになる。

【0042】なお、このインストーラ(またはセットアッププログラム)401はDVD-RAMドライブ303の一部として考えることもでき、その意味で、メディ

アキーブロックMKB__SD2の書き込みを行うのはDVD-RAMドライバ303であるということもできる。

【0043】(1) インストーラ(またはセットアッププログラム)401は、DVD-RAMメディア用のデバイスキー(DevKEY__RAM)を有している。インストーラ(またはセットアッププログラム)401は、デバイスキー(DevKEY__RAM)とDVD-RAMメディア201のリードインエリアに記録されているメディアキーブロック(MKB__RAM)とを用いて、DVD-RAMメディア201との間の認証を行い、これによってメディア固有キー(Kmu__RAM)を得る(プロセス#11)。この場合、まず、デバイスキー(DevKEY__RAM)によってメディアキーブロック(MKB__RAM)を参照することにより、メディアキーKmが得られ、次いで、そのメディアキーKmとDVD-RAMメディア201のリードインエリアに記録されているDVD-RAMメディア固有のメディアID(Media ID2)とからメディア固有キー(Kmu__RAM)が生成されることになる。

【0044】(2) インストーラ(またはセットアッププログラム)401は、WEBサーバ501からSDメモ리카ード用の最新のメディアキーブロック(MKB__SD2)を取得する(プロセス#12)。

(3) インストーラ(またはセットアッププログラム)401は、メディアキーブロック(MKB__SD2)をDVD-RAMメディア固有のメディア固有キー(Kmu__RAM)で暗号化し(Kmu__RAM[MKB__SD2])、それをDVD-RAMメディア201のユーザデータエリアに書き込む(プロセス#13)。

【0045】(コンテンツの書き込み)次に、図5を参照して、DVD-RAMメディア201へのコンテンツの書き込み動作を説明する。ここでは、SDメモ리카ード101に記録されているコンテンツをDVD-RAMメディア201にコピーまたは移動する場合を想定する。

【0046】(1) アプリケーションプログラム301は、デバイスキー(DevKEY__SD)とSDメモ리카ード101に記録されているメディアキーブロック(MKB__SD1)とを用いて、SDメモ리카ード101との間の認証をSDドライバ302を介して行い、これによってメディア固有キー(Kmu__SD1)を得る(プロセス#21)。この場合、まず、デバイスキー(DevKEY__SD)によってメディアキーブロック(MKB__SD1)を参照することにより、メディアキーKmが得られ、次いで、そのメディアキーKmとSDメモ리카ード101に記録されているSDメモ리카ード固有のメディアID(Media ID1)とからメディア固有キー(Kmu__SD1)が生成されることになる。

【0047】(2) アプリケーションプログラム301は、SDドライバ302を介してSDメモ리카ード101から暗号化されたタイトルキー(Kmu__SD1[Kt])を読み出し、それをメディア固有キー(Kmu__SD1)で復号してKtを得る(プロセス#22)。

【0048】(3) アプリケーションプログラム301は、DVD-RAMメディア201との認証要求をDVD-RAMドライバ303に発行する。これに回答して、DVD-RAMドライバ303は、デバイスキー(DevKEY__RAM)とDVD-RAMメディア201のリードインエリアに記録されているメディアキーブロック(MKB__RAM)とを用いて、DVD-RAMメディア201との間の認証を行い、これによってメディア固有キー(Kmu__RAM)を得る(プロセス#23)。この場合、まず、デバイスキー(DevKEY__RAM)によってメディアキーブロック(MKB__RAM)を参照することにより、メディアキーKmが得られ、次いで、そのメディアキーKmとDVD-RAMメディア201のメディアID(Media ID2)とからメディア固有キー(Kmu__RAM)が生成されることになる。

【0049】(4) DVD-RAMドライバ303は、DVD-RAMメディア201に暗号化されて記録されているメディアキーブロック(Kmu__RAM[MKB__SD2])を読み出し、それをメディア固有キー(Kmu__RAM)で復号して、MKB__SD2を得る(プロセス#24)。そして、MKB__SD2をアプリケーションプログラム301に渡す。

【0050】(5) (6) アプリケーションプログラム301は、DVD-RAMドライバ303からMKB__SD2を取得すると、そのMKB__SD2とデバイスキー(DevKEY__SD)とを用いて、DVD-RAMメディア201との間の認証を行い、これによってメディア固有キー(Kmu__SD2)を得る(プロセス#25)。この場合、まず、デバイスキー(DevKEY__SD)によってメディアキーブロック(MKB__SD2)を参照することにより、メディアキーKmが得られ、次いで、そのメディアキーKmとDVD-RAMメディア201のメディアID(Media ID2)とからメディア固有キー(Kmu__SD2)が生成されることになる。

【0051】(7) アプリケーションプログラム301は、プロセス#22で得られたタイトルキーKtをメディア固有キー(Kmu__SD2)で暗号化し、Kmu__SD2[Kt]を得る。そして、そのKmu__SD2[Kt]を、DVD-RAMドライバ303を介してDVD-RAMメディア201に書き込む(プロセス#26)。

【0052】(8) アプリケーションプログラム301は、暗号化されたコンテンツ(Kt[Content])

t])をSDメモ리카ード101から読み込み、それをDVD-RAMドライバ303を介してDVD-RAMメディア201に書き込む。

【0053】(コンテンツの再生)次に、図6を参照して、DVD-RAMメディア201に記録されているコンテンツをアプリケーションプログラム301が再生する場合の動作について説明する。

【0054】(1)アプリケーションプログラム301は、DVD-RAMメディア201との認証要求をDVD-RAMドライバ303に発行する。これに回答して、DVD-RAMドライバ303は、デバイスキー(DevKEY_RAM)とDVD-RAMメディア201のリードインエリアに記録されているメディアキーブロック(MKB_RAM)とを用いて、DVD-RAMメディア201との間の認証を行い、これによってメディア固有キー(Kmu_RAM)を得る(プロセス#31)。この場合、まず、デバイスキー(DevKEY_RAM)によってメディアキーブロック(MKB_RAM)を参照することにより、メディアキーKmが得られ、次いで、そのメディアキーKmとDVD-RAMメディア201のメディアID(Media ID2)とからメディア固有キー(Kmu_RAM)が生成されることになる。

【0055】(2)DVD-RAMドライバ303は、DVD-RAMメディア201に暗号化されて記録されているメディアキーブロック(Kmu_RAM[MKB_SD2])を読み出し、それをメディア固有キー(Kmu_RAM)で復号して、MKB_SD2を得る(プロセス#32)。そして、MKB_SD2をアプリケーションプログラム301に渡す。

【0056】(3)(4)アプリケーションプログラム301は、DVD-RAMドライバ303からMKB_SD2を取得すると、そのMKB_SD2とデバイスキー(DevKEY_SD)とを用いて、DVD-RAMメディア201との間の認証を行い、これによってメディア固有キー(Kmu_SD2)を得る(プロセス#33)。この場合、まず、デバイスキー(DevKEY_SD)によってメディアキーブロック(MKB_SD2)を参照することにより、メディアキーKmが得られ、次いで、そのメディアキーKmとDVD-RAMメディア201のメディアID(Media ID2)とからメディア固有キー(Kmu_SD2)が生成されることになる。

【0057】(7)アプリケーションプログラム301は、DVD-RAMドライバ303を介してDVD-RAMメディア201から暗号化されたタイトルキー(Kmu_SD2[Kt])を読み出し、それをメディア固有キー(Kmu_SD2)で復号してKtを得る(プロセス#34)。

【0058】(8)アプリケーションプログラム301

は、DVD-RAMドライバ303を介してDVD-RAMメディア201から暗号化されたコンテンツ(Kt[Content])を読み出し、それをKtで復号して再生する(プロセス#35)。

【0059】以上のように、本実施形態においては、DVD-RAMメディア/ドライブ用の制御プログラムであるDVD-RAMドライバ303によってSDメモ리카ード用のメディアキーブロックMKB_SDをDVD-RAMメディア201上に記録し、その記録したメディアキーブロックMKB_SDを用いてDVD-RAMメディア201との認証をアプリケーションプログラム301に実行させることにより、SDメモ리카ード用のデバイスキーDev KEY_SDで、DVD-RAMメディアも扱うことが可能となる。よって、著作権保護機能に対応した正当な記録メディアであればその種別を意識することなく、それら記録メディアを透過的に扱うことが可能となる。

【0060】特に、SDメモ리카ード用のメディアキーブロックMKB_SDを、MKB_RAMとの認証によって得たKmu_RAMによって暗号化した状態でDVD-RAMメディア201に書き込むことにより、結果的にメディアキーブロックMKB_SDとMKB_RAMとが関連づけられた形となるので、MKB_SDの秘匿化を図ることが可能となる。

【0061】なお、本実施形態では、最新のメディアキーブロックMKB_SD2を取得してDVD-RAMメディアに記録したが、これは排除すべきデバイスキーの増加に対応させるためである。したがって、SDメモ리카ードに記録されているMKB_SDが最新のもの、あるいは比較的新しいものであれば、それをDVD-RAMメディアに記録するようにしても良い。

【0062】また、コンテンツの暗号化鍵であるタイトルキーをメディア固有キーを用いて暗号化するようにして、メディア固有キーをタイトルキーとして使用し、コンテンツ自体をメディア固有キーを用いて暗号化するようにしてもよい。

【0063】また、DVD-RAMメディアとSDメモ리카ードに限らず、他の各種記録メディアにも同様の方法を適用することができる。

【0064】さらに、本実施形態は、PCに限らず、セットトップボックス、ゲーム機、オーディオ/ビデオプレイヤーなど、マイクロプロセッサを搭載したあらゆるデータ処理装置(コンピュータ応用機器)に適用することができる。

【0065】また、本実施形態で説明したコンテンツ管理方法の手順を記述したコンピュータプログラムを記録媒体を通じてコンピュータまたはコンピュータ応用機器に導入することにより、本実施形態と同様の効果を容易に得ることができる。

【0066】

【発明の効果】以上説明したように、本発明によれば、ある特定のメディア種別に対応したデバイス識別情報によって他のメディア種別の記録メディアを扱えるようになり、著作権保護機能に対応した正当な記録メディアであればその種別を意識することなく、それら記録メディアを透過的に扱うことが可能となる。よって、拡張性、互換性に優れたコンテンツ管理を実現できる。

【図面の簡単な説明】

【図1】本発明の一実施形態に係るコンテンツ処理システムの基本構成を示すブロック図。

【図2】同実施形態のシステムで使用されるメディアキーブロックとデバイスキーとの関係を説明するための図。

【図3】同実施形態のシステムで使用されるコンテンツの暗号化／復号化の原理を説明するための図。

【図4】同実施形態のシステムで行われるメディアキーブロックの書き込み処理の手順を説明するための図。

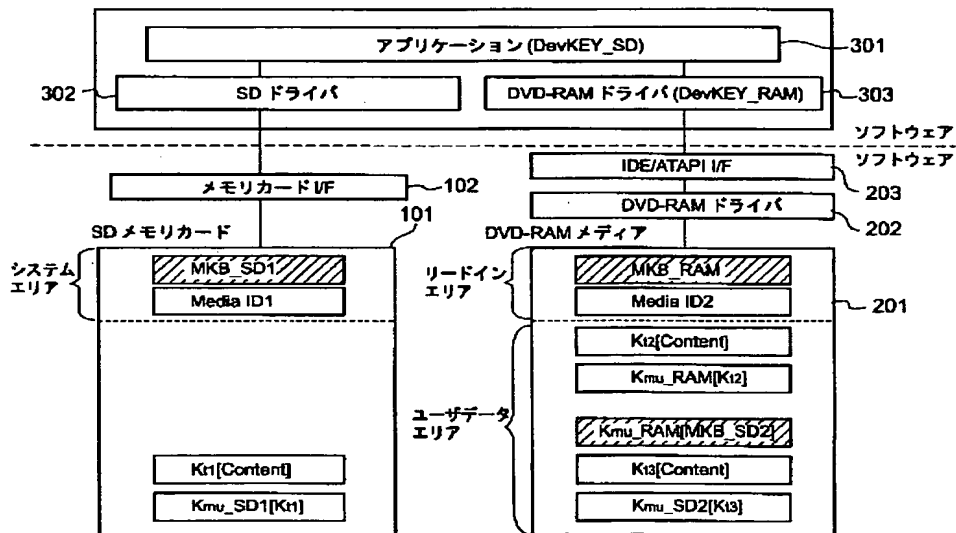
【図5】同実施形態のシステムで行われるコンテンツ書き込み処理の手順を説明するための図。

【図6】同実施形態のシステムで行われるコンテンツ再生処理の手順を説明するための図。

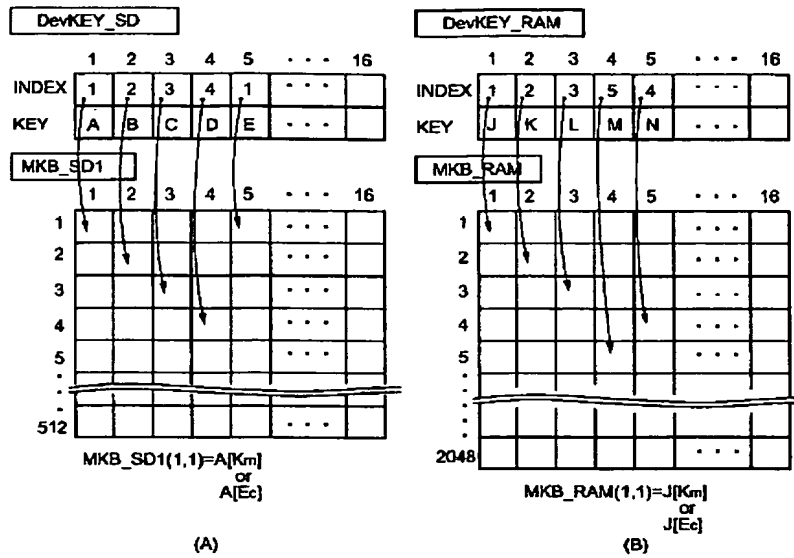
【符号の説明】

- 101…SDメモリカード
- 102…メモリカードインターフェース
- 201…DVD-RAMメディア
- 202…DVD-RAMドライブ
- 203…IDE/ATAPIインターフェース
- 301…アプリケーションプログラム
- 302…SDドライブ
- 303…DVD-RAMドライブ

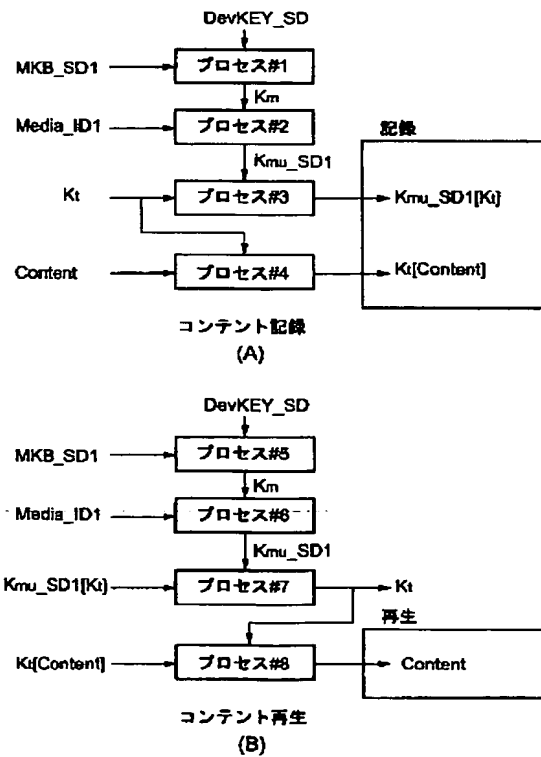
【図1】



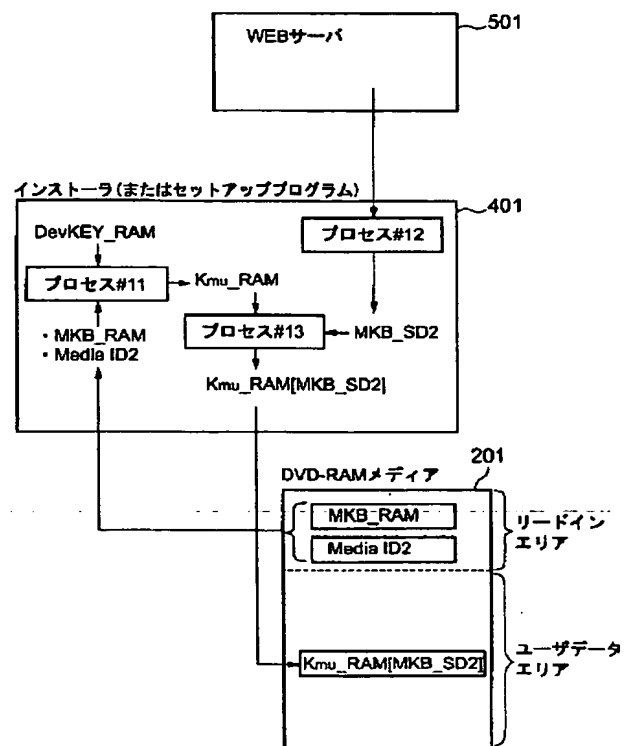
【図2】



【図3】



【図4】



The diagram illustrates the data and control flow in a DVD player system. It is divided into four main functional blocks:

- SDメモリカード (SD Memory Card) 101:** Contains MKB_SD1, Media ID1, and Ki[Content]. It provides data to the SDドライバ (301) via lines ① and ②.
- SDドライバ (SD Driver) 301:** Contains プロセス#21, プロセス#22, and Kmu_SD1. It receives data from the SDメモリカード and outputs Kmu_SD1[Ki] to the DVD-RAMドライバ (302) via line ③.
- DVD-RAMドライバ (DVD-RAM Driver) 302:** Contains DevKEY_RAM, プロセス#23, プロセス#24, Kmu_RAM, and MKB_SD2. It receives Kmu_SD1[Ki] and outputs Kmu_RAM[MKB_SD2] to the DVD-RAMメディア (201) via line ④.
- DVD-RAMメディア (DVD-RAM Media) 201:** Contains MKB_RAM, Media ID2, Kmu_RAM[MKB_SD2], Media ID2, and Ki[Content]. It receives data from the DVD-RAMドライバ and outputs Kmu_SD2[Ki] back to the SDドライバ via line ⑦.

Control and data paths are indicated by arrows and numbered lines (①-⑦). The system also includes a DevKEY_SD block at the top, which provides a DevKEY signal to the SDドライバ and the DVD-RAMドライバ.

The diagram illustrates the system architecture across three main layers:

- アプリケーション (Application) Layer (301):** Contains **DevKEY_SD**, **プロセス#33** (Process #33), **プロセス#34** (Process #34), and **プロセス#35** (Process #35). Data flows from **DevKEY_SD** to **プロセス#33**, which outputs **Kmu_SD2**. **プロセス#33** also receives **MKB_SD2** and **Media ID2**. **プロセス#34** receives **Kmu_SD2** and outputs **Ki**. **プロセス#35** receives **Ki** and outputs **Content**.
- DVD-RAMドライバ (DVD-RAM Driver) Layer (303):** Contains **DevKEY_RAM**, **プロセス#31** (Process #31), and **プロセス#32** (Process #32). **DevKEY_RAM** outputs **Kmu_RAM** to **プロセス#31**. **プロセス#31** outputs **Kmu_RAM** to **プロセス#32**. **プロセス#32** outputs **MKB_SD2** to the Application layer. **プロセス#32** also receives **Kmu_RAM[MKB_SD2]** from the Media layer.
- DVD-RAMメディア (DVD-RAM Media) Layer (201):** Contains **MKB_RAM**, **Media ID2**, **Kmu_RAM**, and **Kmu_SD2**. It receives **①** (MKB_RAM), **②** (Media ID2), and **③** (Kmu_RAM) from the Driver layer. It outputs **④** (MKB_SD2), **⑤** (Media ID2), and **⑥** (Kmu_SD2) to the Application layer.

Arrows indicate the direction of data flow between components and layers.